Making Data Subjects aware of their rights and capable of protecting themselves, Conf. on the rights and responsibilities of Data Subjects, Prague, 14-15 octobre 2004.

Dinant, Jean-Marc; Poullet, Yves

Publication date:
2004

Document Version
Publisher's PDF, also known as Version of record

DP (2004) Report POULLET

THE COUNCIL OF EUROPE AND
THE OFFICE FOR PERSONAL DATA PROTECTION
OF THE CZECH REPUBLIC

CONFERENCE ON THE
RIGHTS AND RESPONSIBILITIES OF DATA SUBJECTS

14 and 15 October 2004
Prague (Czech Republic)

MAKING DATA SUBJECTS AWARE OF THEIR RIGHTS AND CAPABLE OF PROTECTING THEMSELVES

Report by Professor Yves Poullet
Dean of the Faculty of Law
FUNDP (Namur/ Belgium)
Director of the Computer Science and Law Research Centre (CRID)
http://www.droit.fundp.ac.be
yves.poullet@fundp.ac.be

1. The question this report addresses is how, in a globalised world, data subjects can be made aware of their rights and responsibilities and contribute to their own protection.

The question itself raises a number of issues to be considered at the outset.

2. Those who defend privacy are concerned about **globalisation**. The new networks are removing the world's frontiers. My curriculum vitae on the Internet is accessible from the four corners of the planet. The visible or invisible trail left by my computer is transmitted over different networks and may be identified and processed in innumerable locations, near and distant, of which I may or may not be aware.

Globalisation creates new dangers, and makes it difficult to establish confidence in distant sites that are sometimes barely identifiable and subject to little or no regulation.

It also equates with the omnipresence and increasing multifunctionality of networks and communication services. The list of networks - G.P.S/RFID/GSM/Wifi/BlueTooth/GRPS/SMS – continues to grow, as does their capacity and interoperability. More and more products are fitted with microchips connecting them to networks and more and more human activities have access to these networks. Read a newspaper, pay a supplier, place a small ad, open one's garage, look for a job or information or simply a street, chat with friends, order a book or a travel ticket, select a film ... barely a single activity falls outside the growing reach of information and communication technologies, in their globalised form.

3. The question suggests two ways of tackling the issue: **greater awareness and empowerment**.

Those who put the question not only want to improve data subjects' passive situation by making them better informed and educated and more aware of their rights but are also seeking means by which those concerned can protect themselves.

Both approaches can be easily justified.

Greater awareness is made necessary by the growing power of computers and networks, which is greatly increasing the potential, qualitative and quantitative, for processing data. Moreover data subjects are generating an ever wider and richer range of data through their use of networks. Finally, and above all, the data that is processed is becoming increasingly difficult to identify or even spot.

Add to this the growing sense among numerous users that they are losing control of their terminal equipment, that is of the object that allows them to connect up to and use the network. Terminal equipment is broadly defined to include any product or component of a product connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks[1]. Although fixed and mobile telephones and PCs come spontaneously to mind, there are also cards and card readers, Radio Frequency Identifiers (RFIDs) and all the telemetric systems for the remote identification of persons or relating objects to identifiable individuals. Referring to these terminals, Dinant[2] speaks of a "change

[1] Directive 1999/5/EC on radio equipment and telecommunications terminal equipment.

[2] J. M. Dinant, draft report on the application of data protection principles to global telecommunications networks, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Provisional Document, Strasbourg, 20th meeting, 28-30 June 2004.

in the social paradigm". He continues: "Telecommunications devices still involve a cause-effect relationship but this is no longer dictated by the user but rather by the equipment designer. In other words, pressing a key no longer brings about an almost mechanical change in the state of the device, a change that, moreover, can generally be perceived (for example, taking the receiver off the hook and hearing the dialling tone or receiving a call and setting off the ringing tone) but constitutes a command to a computer programme that can do what the user wants autonomously, according to whether and how the programmer has so decided. Moreover, this action is in general partly invisible to the naked eye."[3].

It is not only terminals that resemble black boxes. The same applies to the vast information and communication systems run by large government departments and private companies. Information is no longer seen in terms of one or two static purposes but as material that can be infinitely recycled within evolving systems to satisfy needs that cannot be identified at the outset or that cannot be satisfied. These wide-ranging information systems see personal data increasingly as items at the disposal of many users for purposes not defined in advance. For example, data on medical prescriptions on health cards may be available for subsequent use to monitor prescribers, to compile public health statistics, to assist reimbursement, for use in emergencies and so on.

4. This raises the second issue of why we should focus on data subjects' active role and make them responsible for their own protection.

As well as multiplying the data generated by data subjects, network interaction gives the latter more opportunity to negotiate the protection of their data, by restricting the uses to which they can be put and the number of users.

This leads on to so-called "privacy enhancing technologies"[4], which in various forms create a sense of user empowerment[5] and try to re-establish a certain balance between data collectors and data subjects.

The result is that from the standpoint of awareness raising and own initiatives data subjects have both rights and obligations. They are entitled to data protection but at the same time have a duty to behave in a way that limits the risk that the data will be misused.

Such an approach, which requires data subjects to contribute to their own protection, is one of the underlying themes of the Council of Europe Recommendation on the protection of Internet data[6].

The problem is that data subjects are in a similar situation to consumers, that is in an economically and technologically weak position. To respond to this, regulations are designed

---

[3] A good example of this user's malaise is provided by cookies, which chat away to each other quite outside the net surfer's control.

[4] Term first used in August 1995 in the joint report of the Ontario Information and Privacy Commission and the Netherlands *Registratiekamer*, *The Path to Anonymity*, Achtergrondstudies en Verkenningen 11, The Hague, 2 volumes, 2nd ed., 1998.

[5] See also the application of this concept to information and communication systems and freedom of expression in M. d' Udekem-Gevers and Y. Poullet, Internet Content Regulation - Concerns from an European User Empowerment Perspective, 17 CL&SR 2001, p. 371 and ff., 18 CL&SR 2002, p.11 and ff

[6] Though in a very qualified manner: see Recommendation No R (99) 5 for the protection of privacy on the Internet, adopted by the Committee of Ministers on 23 February 1999: "Use of the Internet places responsibilities on each of your actions and poses risks to privacy. It is important to behave in a way that provides protection to yourself and promotes good relations with others."

to protect the weaker party, the data subject, against the stronger, the data file controller, on whom it imposes certain responsibilities and obligations. Admittedly it is possible to imagine that at some time in the future certain legal obligations might also be imposed on data subjects to limit the risks to themselves, but this implies that file controllers will also comply fully with the relevant regulations. To take an example from another field, wearing seatbelts was only made compulsory for drivers after manufacturers had been required to fit them in their cars. We will return to this illustration[7].

5. The original question, as currently phrased, offers an insight into the questioner's hopes as well as fears. It suggests that internetworking and other technological solutions can enable data subjects to accept responsibility for protecting themselves against the new threats to privacy from the globalisation, opacity and increasing capacity of networks.

6. To answer the question, we must first describe the contributions that each form of regulation can make. We will consider firstly (section I) the relative merits of public regulation, self-regulation and technology, before concluding that joint regulation is what is required.

Section II looks at the need for new principles on which to base new regulations, to take account of the changed context. Efforts to make data subjects more aware of modern information systems and accept responsibility for their response seem to have taken on a new dimension, which calls for new forms of regulation, irrespective of their source.

Finally section III looks at the contribution that each component of the information society can make to achieving a solution. Traditionally, privacy legislation has been confined to three parties: data controllers, data subjects and those responsible for monitoring and balancing the interests of the two protagonists, the public data protection authorities as defined in data protection legislation[8].

Recent legislation and regulations reveal the appearance of new parties with perhaps an even more decisive role, namely consumers' associations and suppliers of telecommunications services, particularly network access suppliers and, above all, manufacturers of terminal equipment.

Section I: Three forms of regulation to inform and empower information and communication service users: legislation, self-regulation and technology – a plea for joint regulation

7. This section will not look in detail at the three forms of regulation traditionally associated with data protection: legislation, self-regulation and technology[9]. We are simply concerned with how the three approaches can help, first separately then in combination, to make data subjects better informed about their rights and better able to exercise them.

---

[7] … for which we are grateful to our colleague Jean Marc Dinant.

[8] The Council of Europe only recognised the importance of the third party very recently, with the opening for signature in November 2001 of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows. The protocol "aims to enforce the effective protection of the individual by requiring the Parties to create one or more supervisory authorities that contribute to the protection of the individual's rights and freedoms with regard to the processing of personal data".

[9] For more information, see in particular J. Reidenberg, Privacy Protection and the Interdependence of Law, Technology and Self-regulation, in *Variations sur le droit de la société de l'information*, Cahier du Crid, n° 20, Bruylant Brussels, 2002, p. 126 and ff.; C.J. Bennett and C.D. Raab, The Governance of Privacy, Ashgate, 2003, p. 12 and f.

A. The law

8. In accordance with Article 8 of Convention No. 108 (Protection of Individuals with regard to Automatic Processing of Personal Data), our data protection legislation grants certain rights to data subjects. These rights offer them a certain control over the image of them that can be presented. Examples include the right to be informed of the existence of a file, the right of access and the right of rectification or erasure.

Modern legislation has tended to expand these rights in line with the growing complexity of information systems. In particular, since European Directive 95/46/EC[10], access to data is no longer seen purely in terms of their content but also of their origin and, above all, the logic involved in their automatic processing. The directive also grants data subjects the right not to be subject to decisions based on automated processing, making it necessary to enter into dialogue with the individuals concerned. More recently, Directive 2002/58/EC[11] has required consent for electronic communications for "direct marketing purposes".

This extension is not confined to new rights for data subjects but also entails new obligations for data controllers. This is illustrated by the recent California Online Privacy Protection Act (OPPA)[12], which requires all Web service suppliers who collect data to establish a Web page including certain information[13].

9. Although these new rights have been enshrined in legislation, their application remains limited, if not non-existent. According to two Eurobarometer polls[14] published by the European Commission in 2003, 49% of firms said that they had received fewer than 10 requests for access in 2000 and 25% said they had had none. The authors of the report on companies' perceptions of data protection legislation conclude that compliance with the law is not a priority since companies receive very few complaints.

This is probably due to data subjects' limited knowledge of the data protection issue and its ramifications (70% of Europeans considered that awareness of personal data protection was low) and of existing data protection legislation (only 32% had heard of the right of access to and correction and erasure of data[15]). We believe that another factor is the relative confidence European citizens have in the measures introduced by their countries, even if they are unaware of their content. In other words government intervention has the perverse effect of making those who should be the first persons concerned – data subjects – feel less personally responsible for their own protection.

---

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data, Official Journal L 281 , 23/11/1995, P. 0031 – 0050.
[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal, 23/11/1995, L 201 P. 0037 – 0047.
[12] Enacted in 2003 and in force since 1 July 2004. It adds new sections (22575-22579) to the Californian Business and Professions Code.
[13] In particular, in addition to information traditionally required by legislation (data controller's identity, types of data collected, purposes for which used), it also requires information tailored more closely to the ephemeral nature of Web sites, such as modification procedures and the date of the Privacy Policy.
[14] See the two Eurobarometer surveys published by the Internal Market Directorate and available on http://europa.eu.int/commm/internal_market/privacy. The first (Special Eurobarometer 196, September 2003) focuses on the views of European citizens, the second (Flash Eurobarometer 147, September 2003), on those of businesses.
[15] And only 7% had used this right of access.

Moreover, ordinary citizens or even their lawyers are likely to be discouraged by the abstract and excessively general wording of data protection legislation. How is someone to interpret abstruse provisions such as one forbidding data controllers from processing data if this is incompatible with the purpose for which the data were initially collected, when he has just received an email from his bank telling him that his accident insurance premium has to go up because of the additional risks arising from his recent job loss or his poor stock market investments, or that he should consider taking out a cheaper insurance with them than with a competitor, whose existence has been highlighted by a bank transfer? Many members of the public find it ironic that legislation to enable them to protect themselves and control their environment is too difficult to understand.

Legislation is therefore, by itself, an inadequate safeguard.

B. Self-regulation

11. Self-regulation as an alternative to public regulation may be a tempting prospect. Privacy policies, in the form of simple commitments, codes of practice and privacy standards[16], drawn up by the industry itself, either alone or under supervision, as in the case of the "Safe Harbour Principles"[17], are flourishing. The advantage for data subjects is that they offer principles that are adapted to the particular circumstances of a company or sector, in a language that is much easier to understand than formal legislation.

The criticisms of self-regulation are well known. The first concerns the absence of safeguards regarding the effectiveness of this form of regulation. A distinction needs to be drawn here between the different types of self-regulation. Privacy commitments are undertakings by individual companies. Privacy codes of practice are laid down at more collective levels, such as an industrial sector. Individual firms accept the principles, and in the event of non-compliance any sanctions that may be imposed by the association that drew up the code. Finally, standards involve an assessment procedure for determining whether those that agree to abide by them do in fact do so. Such a procedure may take the form of certification[18] that data protection conforms with the agreed principles and the awarding of a label[19]. More general standards subject to checks and audits may also be developed[20].

Remedies against non-compliance may be improved by setting up alternative dispute resolution (ADR) machinery[21] that is readily accessible, has clearly identifiable powers and is capable of producing appropriate and constructive solutions.

---

[16] On the difference between these forms of self-regulation see C.J. Bennett and C.D. Raab, The Governance of Privacy, Ashgate, 2003, p. 12 ff.

[17] See Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ L 215 of 25.8.2000). The Principles have been negotiated with the US government and declarations of compliance are published on the Department of Commerce official site. For the Principles as a means of joint regulation, see Y. Poullet, *Les Safe Harbor Principles; Une protection adéquate*, on http://www.droit-technologie.org.

[18] For example, by Trust-e, BBB Online, Privacy Programme and Webtrust.

[19] See J.R. Reidenberg, *Adapting Labels and Filters for Data Protection*, Cybernews, 1997, III, 6.

[20] Examples include the Canadian Model Code for the Protection of Personal Information, approved by the Standards Council of Canada in March 1996. More recently there have been discussions in the ISO.

[21] For more on ADR and its application to personal data protection, see ***. The Safe Harbor Principles make the establishment of ADR a key element of the enforcement system. "Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are

This means that complaints of lack of effectiveness may be valid for "weak" forms of self-regulation but need to be substantially qualified for its more advanced forms. However, the growing number of labels, whose scope and sometimes content is becoming increasingly difficult to assess, is certainly open to criticism. Uncontrolled self-regulation means that data subjects must themselves decide on its value[22].

12. A second criticism concerns the risks posed by the "voluntary" nature of self-regulation. It might be argued that where undertakings are non-existent or do not add up to very much, data subjects will opt for competing firms that have accepted more binding self-regulation that offers greater protection. Such an argument holds little water when it is recognised that in practice the choice does not exist and that in any case privacy protection is hardly a key criterion in determining which firm an individual will choose.

A third criticism relates to the nature of the protection offered. Standards are often weak because they are drawn up exclusively by data controllers, who are anxious not to add too much to their existing burdens.

C. Technological solutions

13. So-called Privacy Enhancing Technologies (PETs)[23] are increasingly being cited as data protection tools, either as a back-up to self-regulatory approaches such as P3P[24] or as a substitute for other forms of regulation, like encryption[25].

Such approaches might be applied to the infrastructure, such as the automatic blocking of connections to countries that fail to comply with data protection rules, to data controllers, to intermediaries, such as the use of filters by special servers to block spam sent by certain types of enterprise, or to data subjects' terminals, such as tools to prevent the sending and receiving of cookies or to negotiate with the data controller.

14. Critics of such tools, whose effectiveness is acknowledged[26], focus on the rules that apply. These rules are often agreed by experts who are not very aware of data protection requirements or are more sensitive to the needs of their industry than to data subjects' interests. When the technologies concerned have to be applied by data subjects themselves, the notion of user empowerment is often something of a myth. How can individuals take

---

not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved ...."

[22] See D.J. Solové, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stanford Law Review (2001), 1393 ff.

[23] H. Burkert, Privacy Enhancing Technologies Typology, Critique, Vision, in P. Agre and M Rotenberg (eds), *Technology and Privacy*, MIT Press, Cambridge, Ma., p. 125-143; L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999, p. 26 and ff; J. Reidenberg, Lex Informatica: the Formulation of Information Policy through Technology, 76 Texas Law Rev., 1998, 552-593, Y. Poullet, Technology and Law: from Challenge To Alliance, Information Quality Regulation: Foundations, Perspectives and Applications, U. Gasser (ed.), Nomos Verlagsgesellschaft, 2004, For a presentation of PETs, see the EPIC site: http://www/epic.org/privacy/tools.html.

[24] See J. Catlett, Technical Standards and Privacy: An open letter to P3P developers; on: http://www.junkblusters.com/standards.html.

[25] On the various encryption protocols and anonymous proxy servers as well as anonymisation tools and the use of pseudonyms, see C.J.Bennett and C.D. Raab, op. cit., p. 148 ff.

[26] See, for example, the conclusions of the PISA project, to which we will return (paragraph ...): "Privacy is probably more effective if transactions are performed by means of technologies that are privacy enhancing …rather than relying on legal protection and self-regulation." (http://dbs.cordis.lu/fep)

responsibility for their own protection when the consequences of their decisions are not clear and they sometimes have no choice in the matter? For example, there are sites that refuse access to users who do not accept cookies. Negotiations via P3P may be insidiously bypassed by data controllers who offer to "pay" for personal data. As Dix notes[27]: "Technology is however no panacea for privacy risks in cyberspace; it cannot replace a regulatory framework or legislation, contracts or code of conduct. Rather it may only operate within such a framework. Privacy by negotiation is therefore no alternative to regulation but a necessary additional tool".

D. Amalgamating the three forms of regulation

15. Probably the best way of improving data subjects' protection and raising their awareness is to draw on and link up all three forms of regulation28. Privacy policies provide a good illustration. A legal obligation to publish a Web page on data protection practice that is properly observed by the company concerned, accessible to users and fully compliant with the legislation in fact requires the use of a number of tools that are not themselves necessarily prescribed in the regulations. Whether or not the company is meeting its legal obligations in practice may be the responsibility of particular certifying bodies or auditors[29], who will then issue it with a form of certification or "trustmark". Industry sectors may themselves propose privacy policy models, to avoid too great a diversity of formats, forms or expression and terminology. Where these do not exist, the law must intervene to settle the various points at issue[30].

Computer applications will be used to guarantee that the privacy policy is fully transparent by automatically opening the relevant Web page and, where appropriate, authorising an expert system to compare data subjects' privacy preferences with the options offered by the data controller and outlined in the privacy policy.

16. The regulation of Web site privacy certification procedures provides another obvious example31. The growing number of certification arrangements is very confusing for Internet users. How much value can be attached to a seal of approval that can be copied and has been issued in a far-off location by an unknown body whose independence is less than obvious, whose ability to monitor sites effectively is dubious and whose power of sanction for non-compliance with certification rules is extremely limited? One response may be for government to establish or initiate a certification system for certifiers, operated by a public authority or a body made up of acknowledged independent figures representing a range of interests[32].

To summarise, it seems clear that what is needed is a mixed system of joint regulation[33] where the law is backed up and given full effect by technical and self-regulation arrangements, which it should actively promote.

---

[27] A. Dix , Infomediaries and Negotiated Privacy Techniques, paper presented to the conference "Computers, Freedom and Privacy" (CPF 2000), 19 April, Toronto, on http://portal.acm.org/citation.

[28] See J.R. Reidenberg, Privacy Protection and the Interdependence of Law, Technology and Self-Regulation, in *Variations sur le droit de la société de l'information*, Cahier du Crid, No. 20, Bruylant Brussels, 2002, p. 126 ff.

[29] Such bodies or auditors might themselves be subject to accreditation based on criteria laid down, or at least approved, by government. The TrustUK trustmark offers an interesting example.

[30] For example, eight US federal regulatory institutions have established the Advanced Notice of Proposed Rulemaking (ANPR) procedure seeking public comment on ways to improve financial institution privacy notices required by the Gramm-Leach-Bliley Act.

[31] On the regulation of certification, see the recommendations of the E-confidence Forum on http://www.jrc.it

[32] One example of such a system to ensure that Web sites satisfy the requirements of consumer protection and privacy legislation is the TrustUK trustmark system. See R. de Bruin (uncompleted).

[33] See Y. Poullet, Technologies de l'information et de la communication et « co-régulation », une nouvelle approche? , in Mélanges Coipel, Kluwer, not yet published.

Section II: New principles to encourage awareness and personal responsibility

17. Those features that are most characteristic of the electronic communications service environment – growing presence and multifunctionality of electronic communications networks and terminals, their interactivity, the international character of networks, services and equipment producers and the absence of transparency in terminal and network functioning – all increase the risk of infringing individual liberties and human dignity.

To counter these risks, certain new principles must be established if data subjects are to be better protected and have more control over their environment. Such control is essential if those concerned are to exercise effective responsibility for their own protection.

This is a first attempt to outline such principles. It is based on a range of material and we have tried to structure it around five main principles, since at this stage we prefer not to speak of new "rights" for data subjects.

A. The principle of encryption and reversible anonymity

18. The encryption of message offers protection against access to the content of communications. The quality varies, as do encryption and de-encryption techniques. Encryption software for installation on users' computers (S/MIME or Open PGP protocols) is now available at a reasonable price. Meanwhile, given its ambiguity, the notion of anonymity should perhaps be clarified, and possible replaced by other terms such as "pseudonymity" or "non-identifiability". What is sought is often not absolute anonymity but rather the functional non-identifiability of the author of a message vis-à-vis certain persons[34]. There are many non-binding documents35 advocating citizens' "right" to anonymity when using new technological services. Recommendation No R (99) 5[36] of the Council of Europe's Committee of Ministers states that "anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy".

19. Those using modern communication techniques must be able to remain unidentifiable by service providers and other third parties intervening during the transmission of the message and by the recipient or recipients of the message, and should have free or reasonably priced access to the means of exercising this option[37]. The availability of readily affordable encryption and anonymisation tools and services is a necessary condition for computer users' exercising personal responsibility.

The anonymity or non-identifiability required is not absolute however. Citizens' right to anonymity has to be set against the higher interests of the state, which may impose restrictions

---

[34] See J. Grijpink and C. Priens, Digital Anonymity on the Internet, New Rules for Anonymous Electronic Transactions?, 17 CL&SR § (2001), p. 378 ff.

[35] See in particular S. Rodota, Beyond the E.U. Directive: Directions for the Future, in *Privacy: New Risks and Opportunities*, Y. Poullet, C. de Terwangne and P. Turner (ed.), Cahier du CRID, Kluwer, Antwerpen, n° 13, p. 211 ff.

[36] Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways, available on the Council of Europe site. See also Recommendation 3/97 of the so-called Article 29 Group: Anonymity on the Internet, and the opinion of the Belgian privacy commission on electronic commerce (No. 34/2000 of 22 November 2000, available on the commission's site: http://www.privacy.fgov.be), which points out that there are ways of authenticating the senders of messages without necessarily requiring them to identify themselves.

[37] See the recommendation of the French national data processing commission that access to commercial sites should always be possible without prior identification (M Georges, Relevons les défis de la protection des données à caractère personnel: l' Internet et la CNIL, in *Commerce électronique- Marketing et vie privée*, Paris, 2000, p.71 and 72.

if these are necessary "to safeguard national security, defence, public security, [and for] the prevention, investigation, detection and prosecution of criminal offences". Striking a balance between the legitimate monitoring of offences and data protection may be possible through the use of "pseudo identities", which are allocated to individuals by specialist service providers who may be required to reveal a user's real identity, but only in circumstances and following procedures clearly laid down in law. Other approaches might include the enforced regulation of terminal equipment, to prevent browser chattering, permit the creation of ephemeral addresses and differentiation of address data according to which third parties will have access to the traffic or localisation data, and the disappearance of global unique identifiers by the introduction of uniform address protocols.

B. The principle of reciprocal benefits

20. This principle would make it a statutory obligation, wherever possible, for those who use new technologies to develop their professional activities to accept certain additional requirements to re-establish the traditional balance between the parties concerned. The justification is simple – if technology increases the capacity to accumulate, process and communicate information on others and facilitates transactions and administrative operations it is essential that it should also be configured and used to ensure that data subjects, whether as citizens or consumers, enjoy a proportionate benefit from these advances.

Several recent provisions have drawn on the proportionality requirement to oblige those who use technologies to make them available for users to enforce their interests and rights.

One example is European Directive 2001/31/EC (the "E-Commerce Directive"), which includes electronic anti-spamming provisions. Similarly, Article 5.3 of Directive 2002/58/EC on privacy and electronic communications even includes the requirement that "... the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information ... and is offered the right to refuse such processing ....".

Legislation of the Freedom of Information variety introduces a similar right to transparency vis-à-vis government by adding further information that the latter is obliged to supply. A Swedish commission[38] has recently recommended legislation that would entitle citizens to monitor their cases electronically from start to finish, including their archiving, and oblige the authorities to adopt a good public access structure, to make it easier for individuals to identify and locate specific documents. There is even draft legislation that would make it possible, one way or another, to link any official documents on which decisions were based to other documents on the case. In other words, a public service that has become more efficient thanks to new technology must also be more transparent and accessible to citizens. Citizens' right of access extends beyond the documents directly concerning them to include the regulations on which a decision was based.

21. It is even possible to imagine that certain of the rights associated with data protection, such as the right to information, the rights of access and rectification and the right of appeal, might soon be enforceable electronically. Many applications could be proposed:

---

[38] P. Seipel, Information System Quality as a Legal Concern, in *Information Quality Regulation: Foundations, Perspectives and Applications*, U.Gasser (ed.), Nomos Verlagsgesellschaft, 2004, p. 248. See also the Swedish commission report by P. Seipel, Law and Information Technology: Swedish Views, Swedish Government Official Reports, SOU 2002, 112.

- it should be possible to apply data subjects' right to information at any time through a simple click (or more generally a simple electronic and immediate action) offering access to a privacy policy, which should be as detailed and complete as the greatly reduced cost of electronic dissemination allows. Such a step must be anonymous as far as the page server is concerned, to avoid any risk of creating files on "privacy concerned" users. In addition, in the case of sites that have been awarded quality labels, it should be obligatory to provide a hyperlink from the label symbol to the site of the body that awarded the label. The same would apply to the declaration of the file controller to the supervisory authority. A hyperlink would be installed between an unavoidable page of any site processing personal data and that of the relevant supervisory authority. Finally, consideration might be given to the automatic signalling of any site located in a country offering inadequate protection;

- in the future, data subjects must be able to exercise their right of access using an electronic signature. It would be obligatory to structure files so that the right of access was easy to apply. Additional information, such as the origin of documents and a list of third parties to whom certain data had been supplied, should be systematically available. As noted earlier[39], increasingly, the personal data accumulated by the vast public and private networks are no longer collected for one or more clearly defined purposes but are stored in the network for future uses that only emerge as new processing opportunities or previously unidentified needs arise. In such circumstances, data subjects must have access to documentation describing the data flows within the network, the data concerned and the various users – a sort of data registry[40];

- it should be possible to exercise the rights of rectification and/or challenge on line to an authority with a clearly defined status responsible for considering or maintaining a list of complaints;

- the right of appeal should also benefit from the possibility of on-line referral, exchange of parties' submissions and other documentation, decisions and mediation proposals.

C. The principle of encouraging technological approaches compatible with or improving the situation of legally protected persons

22. Recommendation 1/99 of the so-called Article 29 Group (the EU Data Protection Working Party)[41], which is concerned with the threat to privacy posed by Internet communications software and hardware, establishes the principle that software and hardware industry products should provide the necessary tools to comply with European data protection rules. In accordance with this third principle, regulators should be granted various powers.

23. For example, they should be able to intervene in response to technological developments presenting major risks. The so-called precautionary principle, which is well established in environmental law, could also apply to data protection.

---

[39] See paragraph 3.

[40] This idea is the subject of two recent Belgian laws that require the establishment of sectoral committees for the networks linked to the National Register (Act of 8 August 1983 establishing a national register of persons, as amended by the Act of 25 March 2003, MB. 28 March 2003, art.12§1) and to the commercial registration authority (Banque Carrefour des entreprises) (Act of 16 January 2003 establishing the authority, MB. 5 February. 2003, article 19§4).

[41] Recommendation on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware.

This can be illustrated by one of the provisions of the EU Directive on privacy and electronic communications. Article 14 states that where required, the Commission may adopt measures to ensure that terminal equipment is compatible with data protection rules. In other words, standardising terminal equipment is another, admittedly subsidiary, way of protecting personal data from the risks of unlawful processing – risks that have been created by all these new technological options. Going further, it is necessary to prohibit so-called privacy killing strategies[42], in accordance with the security principle enshrined in Article 7 of Council of Europe Convention 108. The obligation to introduce appropriate technical and organisational measures to counter threats to data privacy will require site managers to make sure that messages exchanged remain confidential, indicate clearly what data is being transmitted, whether automatically or by hyperlink, as is the case with cybermarketing companies, and make it easy to block such transmission.

This security obligation will also require those who process personal data to opt for the most appropriate technology for minimising or reducing the threat to privacy. This requirement clearly has an influence on the design of smart cards, particularly multifunctional cards[43], such as identity cards.

Another example of the application of this principle concerns the structuring of medical files at various levels, as recommended by the Council of Europe.

24. It might be possible to go further by recommending the development of privacy enhancing technologies, that is tools or systems that take more account of data subjects' rights. Clearly, the development of these technologies will depend on the free play of the market but the state must play an active part in encouraging privacy compliant and privacy enhancing products by subsidising their research and development, establishing equivalent voluntary certification and accreditation systems and publicising their quality labels, and ensuring that products considered necessary for data protection are available at affordable prices.

D. The principle of full user control of terminal equipment

25. The justification for this principle is obvious. Since these terminals can enable others to monitor our actions and behaviour, or simply locate us, they must function transparently and under our control. Article 5.3 of Directive 2002/58/EC, cited above, offers a first illustration of this point. Those concerned must be informed of any remote access to their terminals, via cookies, spyware or whatever, and be able to take easy and effective countermeasures, free of charge. Directive 2002/58/EC also establishes the rule that users of calling and connected lines can prevent the presentation of the calling line identification.

Going beyond these examples, we would also argue that all terminal equipment should be configured to ensure that owners and users are fully informed of any data flows entering and leaving, so that they can then take any appropriate action.

Similarly, as is already the case under some legislation, possession of a smart card should be accompanied by the possibility of read access to the data stored on the card.

---

[42] Expression used by J.M. Dinant, Law and Technology Convergence in the Data Protection Field, in *E-commerce Law and Practice in Europe*, I. Walden and J. Horne, Woodhead Publishers Ld, Cambridge, 2002, Chapter 8.2

[43] On the privacy compliant design of multi-application cards, see E. Keuleers and J.M. Dinant, Multi-application smart card schemes, 19, CL&SR, 4 2003, 480 and ss; 20, CL&SR, 1, 2004, 22 and ss.

User control also means that individuals can decide to deactivate their terminals once for all, and at any time. This is important as far as Radio Frequency Identifiers (RFIDs) are concerned. Data subjects must be able to rely on third parties[44] that vouch that such technical means of remote identification have been fully deactivated.

26. Users may well apply this principle to firms that are not necessarily covered by traditional data protection rules because they are not responsible for data processing. Examples include suppliers of terminal equipment and many forms of browser software that can be incorporated into terminals to facilitate the reception, processing and transmission of electronic communications. This point will be considered further in Section III.

The principle also applies to public and private standard setting bodies concerned with the configuration of such material and equipment.

The key point is that the products supplied to users should not be configured in such a way that they can be used, whether by third parties or the producers themselves, for illicit purposes. This can be illustrated by a number of examples:

- a comparison of browsers available on the market shows that chattering between them goes well beyond what is strictly necessary to establish communication;

- browsers differ greatly in how they receive, eliminate and prevent the sending of cookies, which means that the opportunities for inappropriate processing will also vary from one browser to another;

- attention should also be drawn to the use of unique identifiers and spyware by suppliers of browser tools and communication software.

More generally, terminal equipment should function transparently so that users can have full control of data sent and received. For example, they should be able to establish, without fuss, the precise extent of chattering on their computers, what files have been received, their purpose and who sent them.

E. The principle that users of certain information systems should benefit from consumer protection legislation

27. The routine use of information and communication technologies, formerly confined to major undertakings, and the rapid development of electronic commerce that has multiplied the number of on-line services have led to a more consumerist approach to privacy. Web surfers increasingly view infringements of their privacy –spamming, profiling, differential charging policies, refusal of access to certain services and so on – from the standpoint of consumers of these new services.

Thus, in the United States the first hesitant steps towards legislation on data protection in the private sector focussed on on-line consumer protection. Reference has already been made to Californian legislation[45] but we should also bear in mind the 1995 Consumer Privacy Act and,

[44] Clearly this refers to accreditation arrangements such as those already described in paragraph 15 (joint regulation) or to approval issued by the authorities to certain undertakings (public regulation).
[45] See paragraph 12.

more recently, the 2000 declaration of the Federal Trade Commission[46], which emphasised the need for privacy legislation to protect on-line consumers. In Europe as in America measures to combat spamming are concerned with both consumers' economic interests and data subjects' privacy.

28. This convergence between consumers' economic interests and citizens' freedoms opens up interesting prospects. It suggests that the right to resort to certain forms of collective action, which is already recognised in the consumer protection field, should be extended to privacy matters. Such an entitlement to "class actions" is particularly relevant in an area where it is often difficult to assess the detriment suffered by data subjects and where the low level of damages awarded is a disincentive to individual actions.

In addition, many other aspects of consumer law could usefully be applied to data protection. Examples are the obligations to provide information and advice, which could be imposed on operators offering services that essentially involve the management or supply of personal data, such as Internet access providers and personal database servers (case-law databases, search engines and so on), the law governing general contractual conditions (applicable to privacy policy) and measures to combat unfair commercial practices and competition.

Finally, providing personal data as a condition of access to a site or an on-line service could be viewed not merely from the standpoint of data protection legislation – does the user's consent meet the necessary requirements and is it sufficient to legitimise the processing in question? – but also that of consumer law, if only in terms of unfair practices in obtaining consent or the major detriment arising from the imbalance between the value of the data secured and that of the services supplied.

Another avenue to be explored is whether consumer product liability for terminals and software can be extended beyond any physical and financial harm caused to include infringements of data protection requirements. How far is the supplier of browser software whose use leads to breaches of privacy objectively liable for data infringements by third parties?

Part III: The role of traditional and new parties in making data subjects aware of their rights and capable of protecting themselves

29. Much has been said about data subjects' obligations. Thanks to information technologies these obligations have taken on a new dimension. The key points are summarised in paragraph III.11 of Recommendation R (99) 5 of the Council of Europe's Committee of Ministers on the protection of privacy on the Internet[47]: "You are responsible for proper use of data. On your introductory page highlight a clear statement about your privacy policy. This statement should be hyperlinked to a detailed explanation of your privacy practice. Before the user starts using services, when he or she visits your site, and whenever he or she asks, tell him or her who you are, what data you collect, process and store, in what way, for what purpose and for how long you keep them. If necessary, ask for his or her consent. At the request of the person concerned, correct inaccurate data immediately and delete them if they are excessive, out of date or no longer required and stop the processing carried out if the user objects to it. Notify the third parties to whom you have communicated the data of any modification. Avoid the hidden collection of data."

---

[46] See the report to Congress "Privacy Online: Fair Information Practices" May 2000, available on the FTC site: http://www.ftc.gov/os/2000/05/index.htm. In the United States, the FTC, which is very active in the consumer protection field, has played a key role in protecting citizens' privacy.

[47] Adopted on 23 February 1999.

30. We will consider at somewhat greater length the duties of a second traditional party: the data protection authorities, who play a key role in enforcing data protection legislation, albeit one that was rather belatedly recognised by the Council of Europe[48]. These authorities have a particular responsibility for assisting data subjects and promoting awareness of data protection rules among both data subjects and data controllers[49].

In Europe, this role is performed by independent administrative authorities. Eurobarometer has already highlighted the minimal impact of these authorities, often characterised by excessive legalism and procedures rather than a genuinely active stance. This is reflected in the criticisms levelled by Flaherty at an international conference of data protection commissioners: more than two-thirds of Europeans (68%) said that they were unaware of these authorities' existence and only 27% claimed to have heard references to them[50].

This is an alarming finding. The failure of these authorities to attract media attention, even when relevant stories hit the headlines, is undoubtedly worth emphasising. But a visit to their sites reveals other shortcomings. Few of them are attractive[51], and few of them allow complaints to be lodged on line[52]. Only a few sites have opened discussion forums on particular themes, or have made the effort to present data protection laws in the form of frequently asked questions (FAQ)[53]. There is also a regrettable absence of links to university, professional, consumer, civil liberties and other sites offering more information[54]. Nor, unfortunately, do these sites include descriptions of technological services and products offering effective protection[55]. One explanation is probably a lack of financial resources, but this may not be the only reason.

To summarise, authorities that are too inward looking need to look to other citizen protection groups with a view to offering and organising joint information and action.

31. Responsibility for educating data subjects and data controllers cannot be limited to data protection authorities. Civil liberties and consumer protection associations obviously have a part to play if the notion of collective remedies is accepted[56], but so do other bodies. The first is identified in Article 4 of Directive 2002/58: "In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk[57] and, where the

---

[48] See the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS, No 181, Strasbourg 8 November 2001).

[49] These roles have been emphasised by the Article 29 Group, particularly in terms of what constitutes adequate protection (See Working Paper No. 12 of 24 July 1998: "Transfers of personal data to third countries: application of articles 25 and 26 of the Community directive on data protection").

[50] Only in the Netherlands, Italy and Sweden had more than one inhabitant in three heard of this authority. Under the circumstances, the Quebec approach of appointing a journalist to head the access to information and data protection commission merits further consideration.

[51] The French CNIL site is an exception.

[52] In this regard, see the various models for lodging complaints proposed by the Federal Trade Commission.

[53] See in particular the Netherlands site: http://www.cbpweb.nl/documenten/faq_wbp_cbp.htm. and the British one: http:// www.informationcommission.gov.uk, which also offers a particularly well constructed video and CD Rom, though unfortunately this is not available on line. The French site offers a demonstration of how Net users are identified when they visit a Web site.

[54] Probably an indication that our authorities are anxious not to appear to be giving priority to certain opinions or institutions.

[55] Something that is offered by EPIC (Electronic Privacy Information Centre), with hyperlinks such as http://www.epic.org.

[56] See paragraph 27.

[57] See paragraph III.2 of Council of Europe Recommendation No. R (99) 5.

risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved."

For example, Internet access providers and mobile and fixed telephone operators are given responsibility for informing the public about the risks attached to using their networks, for combating privacy killing technologies and, at the same time, for promoting appropriate privacy enhancing ones. Access providers' role is critical, since they are the obligatory interface between users and the network. They are therefore asked[58] to "inform users about technical means which they may lawfully use to reduce security risks to data and communications", to "use appropriate procedures and available technologies, preferably those which have been certified, to protect the privacy of the people concerned , ..., especially by ensuring data integrity and confidentiality as well as physical and logical security of the network and of the services provided over the network", and to inform users "about the possibilities of using [Internet] services and paying for them in an anonymous way". They should set up hotlines for subscribers to submit complaints about breaches of privacy and sign a code of conduct requiring them to block access to sites that fail to meet personal data requirements, irrespective of the site's location.

32. Three other groups of participants in the process have already been mentioned. First there are all the trusted intermediaries whose activities are in principle market governed. These are the infomediaries that act as the interface between data subjects and controllers and reassure data subjects that data protection requirements are being met through an accreditation and certification process and by offering anonymisation and filtering services and negotiating with data controllers. Their activities deserve to be better known and should be encouraged by the authorities[59].

Then there are the manufacturers and developers of the hardware and software that make up the terminal equipment, as well as those responsible for the protocols and technical standards used to transmit information over the network. They should ensure that the configuration of their products and their standards[60]:

- meet legal requirements, for example by transmitting via Internet browsers the minimum information necessary for connection and by adopting appropriate safety standards;

- permit the application of the principles identified in Part II, for example direct user access to his or her personal data or an automatic right of challenge;

- improve the level of protection of personal data.

33. Finally there is the state, which has a responsibility, according to the Council of Europe, for promoting its citizens' rights. This means that it cannot confine itself to investigating and prosecuting abuses. This points to certain conclusions:

---

[58] Recommendation No. R (99) 5, paragraph III, 3, 1 and 4.

[59] For example, via research contracts to permit the development of new services and products. PISA (Privacy Incorporated Software Agent), a project subsidised by the EU's fifth framework programme, offers a good example. For more on this programme, and a comparison of the PISA and P3P approaches (with the former aimed at re-establishing equality between data subjects and their Web sites) see http://www.tno.nl/instit/fel/pisa and Borking and Raab, Laws, PETS and other Technologies for Privacy Protection, JILT, 2001, p. 1 ff (also available on http://elj.werwick.ac.uk/filt/01-1/borking .html.)

[60] See Opinion No. 34/2000 of the Belgian Commission on data protection and electronic commerce.

- educating and informing data subjects cannot just be left to the data protection authorities. When schools are instructing their pupils in the use of information and communication technologies they must also introduce them to the very principles of data protection;

- data controllers should be made aware of their responsibilities through university and other training modules for data protection staff[61], or more generally "security officials"[62], in both government and business. The aim is to make data protection a core element of government and business activity;

- the state has a duty to promote new services and products to assist other forms of regulation and ensure that all those involved in regulation are properly co-ordinated. In the case of technological developments, it also has a duty of precaution.

Whenever new technologies are introduced, particularly ones linked to the use of communication networks, their impact on fundamental liberties must be assessed. Such technology assessments[63] should be accompanied by public debates organised by the data protection authorities and might lead to decisions to suspend development. Clearly, the state can only play such a role if it has an active presence in the normally purely private organisations where decisions on future technological developments are taken[64].

Finally, where the state is itself responsible for data processing, it must not only abide by its own regulations but also encourage approaches that strengthen data subjects' rights. With the advent of e-government and one-stop services, it seems only natural to use existing network applications to offer citizens electronic access to their case files, information on where the data came from and who has had access to it, and an easy-to-understand description of the intra-governmental communication systems involved in dealing with their cases. Government Web sites explaining the different administrative purposes for which data is processed and how the relevant information systems operate and hotlines for receiving complaints and initiating mediation are models that could also be taken up by the private sector.

Conclusions

In the introduction, I referred to the difficulties that the very title of this report presented. The call for greater awareness and more responsibility in the hands of data subjects suggests that at a time of double globalisation[65] of information and communication technologies data subjects' ability to control the use of information about them has significantly diminished.

The challenge is posed by the "black box" represented by increasingly complex and "intelligent" terminals and transnational information systems with limitless processing capacity.

By itself, the law offers limited opportunity for returning even a modicum of control to users. Citizens have little knowledge of the rights that the law so generously grants them but in

[61] See the Belgian delegation's proposals to the conference of data protection commissioners in Buenos Aires.
[62] It cannot be stressed too often that data protection means much more than just ensuring the security of data. As well as maintaining data confidentiality, it is also concerned with the balance between data controllers' and data subjects' interests.
[63] See , D. Flaherty, Privacy Impact Assessments: An essential Tool for Data Protection, 7 PLPR (2000), p. 85 ff.
[64] We have in mind IETF, W3C and ICANN. For more on these organisations, see P. Trudel (ed.), *Droit du cyberespace*, Montreal, Thémis, 1997; J. Berleur, Y. Poullet, Quelles régulations pour l'Internet, Gouvernance de la société de l'information, Cahier du CRID, n° 22, Bruylant, Brussels, p. 133 ff.
[65] Globalisation in the sense that networks are becoming increasingly international and are converging, but also because all our activities are gradually being digitally recorded.

addition data controllers have little incentive to comply with legislation that is so rarely invoked. This is not to criticise the law as such but it does mean that self-regulation and technological solutions are required to enforce and strengthen those rights. The answer is joint regulation, in other words a fruitful dialogue between the various regulatory approaches.

To repeat, the law is necessary. It provides a framework for self-regulation and a yardstick by which the latter may be assessed and judged. Besides, users cannot be simply abandoned, without knowing which form of regulation to trust. The market can only be a good guide if it is transparent and "consumers" are capable of distinguishing data protection factors from other criteria. The user empowerment that certain technologies offer will remain a myth if it is not subject to legal oversight.

Joint regulation calls for new players who will help to raise awareness and offer users real opportunities to control their environment. Examples are organisations that certify Web sites and other infomediaries. Joint regulation should encourage the development of new "safe" technologies and make them available to both users and intermediaries such as Internet access providers. Anonymisation software and services offer good illustrations.

This latter point and the accompanying example reflect two of the new principles we are advocating. What are the others? For data subjects to exercise control over modern information systems' presentation of their image their terminals must operate totally transparently, the emphasis must be on information that is needed for specific purposes rather than to generate a multiple processing capacity and data must be properly documented – origin, users, justification and how and where it circulates.

The purpose of these principles is to offer every individual all that is necessary for them to understand their computer environment, particularly within their own household. They should have full control over tools whose use leaves them open to the gaze of others.

If users are to acquire such control, they will need support from various quarters. We have argued strongly that data protection authorities should be more attentive to the public and offer them more user-friendly information. The state has an educational role to play, towards both data controllers and data subjects, aimed at promoting new tools and new professional skills. We also believe that as the necessary interface between data subjects and the Internet, access providers must provide information on the risks involved and ways of countering them. Finally, terminal equipment manufacturers clearly have responsibilities to meet.

In this way we can make the information highway more secure, with properly signposted communications networks and traffic intersections, vehicles fitted with the necessary safety equipment and drivers who are fully aware of the risks involved and reliably equipped to avoid the dangers. It only remains for these drivers to accept their responsibilities and take an active part in securing their own protection.